e-mail

O correio eletrônico certamente é a aplicaçao mais usada na internet, embora não seja a maior geradora de tráfego. A comúnicaçao interpessoal é primordial, e um sistema operacional servidor de rede deve necessariamente implementar um serviço de correio via TCP/IP.

Imagine você escrevendo uma carta em papel, como em 1365. Você termina, assina, pensa bem no que vai mandar para o destinatário (será que ela vai entender ‘ teus cabelos são mais fascinantes que uma fila de pacotes processada no roteador...’). Bom, você fecha o envelope põe o endereço do remetente, do destinatário, chama seu cão para lamber o selo, cola o selo e envia pela caixa coletora.

Mandar um e-mail é bem parecido. Você apenas troca a caneta e o papel pelo computador. O correio convencional transporta envelopes reais, enquanto o sendmail transporta mensagens eletrônicas em envelopes eletrônicos.

Quando a destinatária é sua vizinha (ela estaria na mesma máquina) somente um posto de correio está envolvido (ou, no caso eletrônico, somente um sendmail rodando localmente). Se a sua amiga mora em Koala Lampur, a mensagem será repassada pelo correio local do seu bairro (sendmail da sua máquina) para um posto distante (sendmail rodando remotamente), que se responsabiliza pela entrega.

Existem algumas vantagens na versão eletrônica dessa história:

- Sua letra sempre sai bonita.
- A entrega tipicamente demora alguns segundos ao invés de alguns dias.
- O re-envio da mensagem é imediato, e ela pode mandar cópias para todas as suas namoradas.
- Se você troca de endereço, basta deixar um arquivo .forward em sua caixa antiga.
- Os endereços são independentes das máquinas, (o sendmail busca por eles de forma dinâmica, sem ter uma tabela estática) que podem ser alteradas a qualquer momento, quebradas, bombardeadas, etc.

Protocolos

0 e-mail, como outros serviços de rede, emprega diversos protocolos. Esses protocolos permitem que máquinas diferentes, frequentemente executando sistemas operacionais distintos e utilizando variados programas de e-mail, possam comúnicar-se via e-mail.

Os protocolos mais utilizados para transferir e-mail de sistema para sistema são o IMAP e o POP

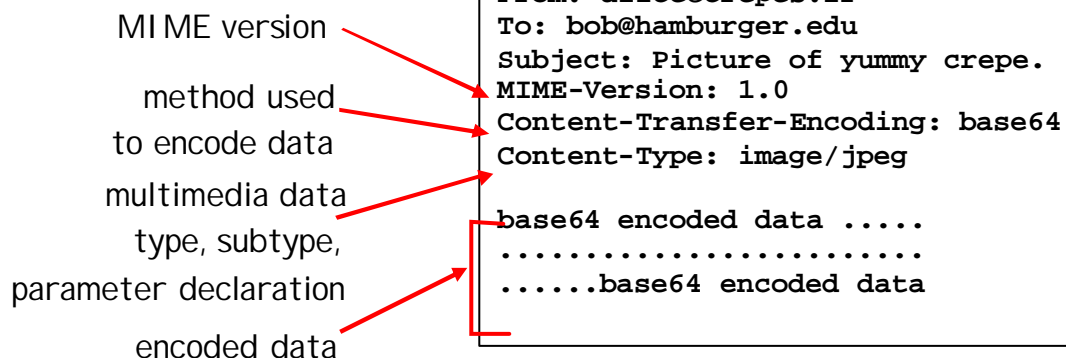
IMAP

The IMAP Connection http://www.imap.org

O Internet Message Access Protocol (IMAP) e um metodo utilizado por aplicacoes clientes de email para acessar mensagens armazenadas remotamente.
Com o IMAP, as mensagens de e-mail permanecem no servidor de correio remoto,
É possível aos usuários:

- **1er**
- **excluir**
- **criar,**
- **renomear**
- **eliminar caixas de correio para armazenar mensagens.**

Além disso, o IMAP e completamente compativel com padroes importantes do sistema de mensagens de Internet,

como as Multipurpose Internet Mail Extensions (MIME) que permitem a recepção de arquivos anexos.

Muitos clientes de e-mail que utilizam IMAP tambem podem ser configurados para armazenar em cache uma copia das mensagens localmente, de modo que os usuários possam navegar e ler mensagens sem estarem diretamente conectados ao servidor IMAP.

0 IMAP e utilizado principalmente por quem acessa e-mail utilizando diversas máquinas.

Além disso, usuários que se conectam a Internet em a uma rede privada via conexão de banda-estreita frequentemente utilizam IMAP

porque somente as informações de cabeçalho de e-mail sao descarregadas primeiro. Isso lhes permite adiar o download de mensagens contendo grandes anexos para que seja feito em um horario no qual a largura de banda limitada nao esteja sendo usada.

Do mesmo modo, as mensagens que os usuários nao quiserem receber podem ser excluidas sem que eles precisem visualizar o corpo de mensagem, evitando a necessidade de ter de fazer seu download por suas conexoes de rede.

Os documentos Request for Comment (RFC) que tratam do IMAP contem detalhes organizados e especificidades sobre como o protocolo foi projetado para trabalhar.

A RFC-1730 primeiro definiu a maneira como o IMAP e utilizado na versao 4

A RFC-2060 discute a implementação do IMAP utilizado coin muitos servidores IMAP, chamada versao IMAP4rev1.

O pacote IMAP do Red Hat Linux permite aos usuários conectarem-se ao sistema e receberem seus e-mails utilizando IMAP.

Conexoes seguras de IMAP sao suportadas por meio da tecnologia Secure Sockets Layer (SSL) incorporada no daemon **`/usr/sbin/imapd`** a fim de permitir o use do arquivo de certificado `/usr/share/ssl/certs/imapd.pem`. O programa stunnel nao é exigido para fornecer criptografia SSL para conexoes de IMAP, embora possa ser utilizado.

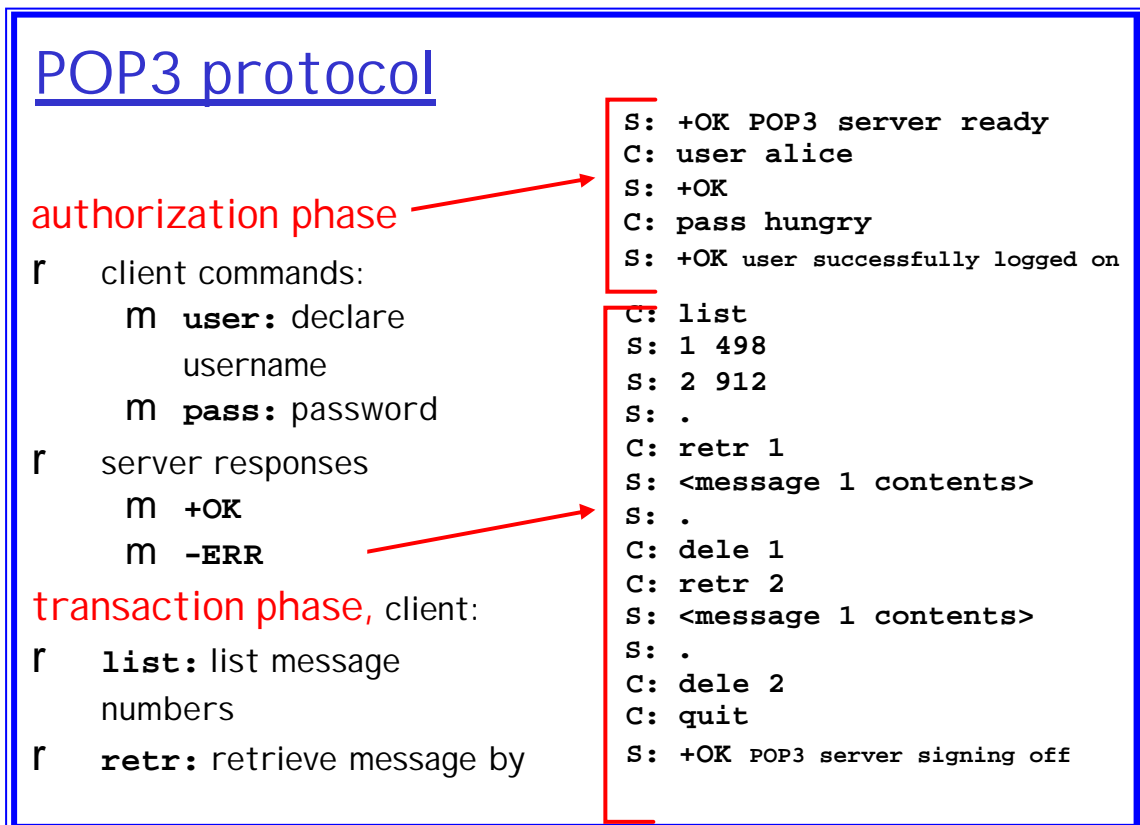
Outros clientes gratuitos, assim como clientes comerciais e servidores IMAP encontram-se disponiveis, muitos dos quais estendem o protocolo de IMAP e fornecem funcionalidade adicional. Uma lista abrangente pode ser localizada em `http://www.imap.org/products/longlist.htm.`

POP

O **Post Office Protocol** (POP) permite que clientes de e-mail façam download de mensagens de e-mail de servidores remotos e salvem essas mensagens em sua máquina local.

A maioria dos clientes de e-mail POP é configurada automaticamente para excluir a mensagem no servidor depois que ela foi transferida com sucesso para o sistema do cliente, embora isso normalmente possa ser alterado.

Para conectar-se a um servidor POP, o cliente de e-mail abre uma conexão TCP para a porta 110 no servidor.

No momento em que a conexão e feita, o servidor POP envia uma saudação para o cliente POP, depois que as duas máquinas trocam comandos e respostas especificadas no protocolo.

Como parte dessa comúnicação, o cliente POP é solicitado a autenticar a si proprio num processo denominado **Estado de Autenticação**,

Nessa fase, são enviados para o servidor POP:

- nome de usuário
- e a senha

Se a autenticação for bem-sucedida, então o cliente POP move-se para o **Estado de Transação**,

onde comandos como `LIST, RETR` e `DELE` podem ser utilizados para

- listar,
- fazer download
- e excluir mensagens do servidor.

As mensagens configuradas para serem excluidas nao sao removidas de fato do servidor ate que o cliente POP envie o comando `QUIT` para terminar a sessao.

Nesse ponto, o servidor POP entra em **Estado de Atualização**, onde:

- exclui as mensagens marcadas
- e limpa quaisquer recursos remanescentes da sessao.

O POP é um protocolo muito mais simples que o IMAP, já que menos comandos sao trocados entre o cliente e o servidor.

O POP funciona melhor para usuários que possuem somente urn sistema para ler e-mail

porque estes fazem download de suas mensagens para essa máquina.

0 POP tambem funciona bem se:

voce nao tiver uma conexão constante:

- com a Internet
- ou com a rede na qual está localizado o seu servidor de correio.

Várias RFCs cobrem o protocolo POP,

mas a RFC-1939 define a estrutura básica do POPS, a versao atual.

Muitos servidores, clientes e diversas outras aplicações POP encontram-se disponiveis para o Linux.

Se preferir urn cliente de e-mail gráfico:

- Mozilla Mail
- Ximian Evolution

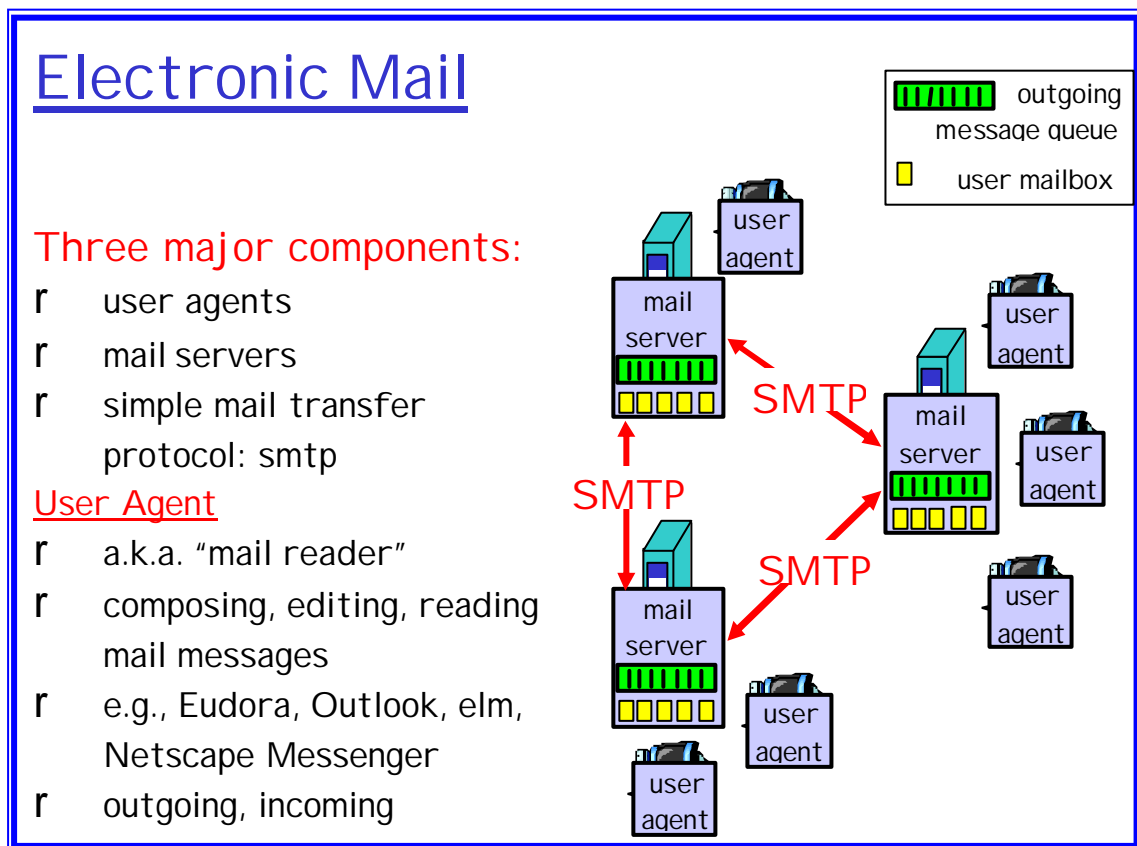
Além disso, outros utilitários, corno o Fetchmail, podem recuperar e-mails via protocolo POP.

Se voce estiver utilizando o Linux corno um servidor de correio, o pacote IMAP instalara os daemons POP2 (ipop2) e POP3(ipop3) no diretório **/usr/sbin/. SMTP**

Enquanto os protocolos IMAP e POP incluem permissao para que OS usuários possam receber e-mails,

o Simple Mail Transfer Protocol (SMTP) e utilizado para enviá-los.

As mensagens despachadas utilizam o SMTP para mover-se da máquina do cliente para o servidor, no caminho rumo ao destino final.

Os servidores de e-mail que tentam mover urna mensagern entre si tambem utilizam o SMTP para essa comúnicação.

O SMTP utiliza a porta 25 no servidor para comúnicação.

Um intercambio SMTP basico comeca quando o sistema que se conecta emitindo um comando MAIL From: *endereço-de-e-mail* para iniciar o processo de transferencia.

0 sistema receptor responde com uma mensagem 250 para informar ao emissor que reconheceu a chegada do comando anterior.

A seguir, o sistema que se conectou inicialmente passa os endereços de e-mail dos destinatarios da mensagem para o sistema receptor,

seguidos por uma mensagem DATA.

Isso informação sistema receptor que a proxima parte da comúnicação sera o corpo real da mensagem de e-mail.

Quando o sistema que se conectou termina a mensagem, coloca um unico ponto (.) em uma linha.

Nesse ponto, a mensagem e considerada como enviada.

O protocolo pode verificar se certos usuarios sao servidos por um servidor particular de correio utilizando o comando VRFY ou expandir uma lista de mala direta utilizando o comando EXPN.

Mensagens de e-mail tambem podem ser transmitidas entre dois servidores SMTP, se ambos os sistemas permitirem tal atividade.

Sample smtp interaction

```
S: 220 hamburger.edu
C: HELO crepes.fr
S: 250  Hello crepes.fr, pleased to meet you
C: MAIL FROM: <alice@crepes.fr>
S: 250 alice@crepes.fr... Sender ok
C: RCPT TO: <bob@hamburger.edu>
S: 250 bob@hamburger.edu ... Recipient ok
C: DATA
S: 354 Enter mail, end with "." on a line by itself
C: Do you like ketchup?
C:   How about pickles?
C: .
S: 250 Message accepted for delivery
C: QUIT
S: 221 hamburger.edu closing connection
```

Ao contrario do IMAP e do POP, o protocolo de SMTP nao necessita de autenticação.

Isso significa que os servidores SMTP permitem a qualquer pessoa na Internet utilizar seu sistema para enviar on transmitir mensagens para grandes listas de destinatarios.

É essa caracteristica do SMTP que torna possivel o spam.

As aplicacoes de SMTP modernas tentam minimizar esse comportamento restringindo a transmissao e permitindo que somente hosts conhecidos enviem mensagens de e-mail.

Try smtp interaction for yourself:

- `telnet servername 25`
- see 220 reply from server
- enter HELO, MAIL FROM, RCPT TO, DATA, QUIT commands

above lets you send email without using email client (reader)

A RFC-821 fornece um esboco do comportamento basico do SMTP, mas diversas extensoes do SMTP, possibilitadas pela RFC-1869, com o passar dos anos adicionaram funcionalidade adicional para esse protocolo disponibilizando novos comandos.

Ao iniciar uma conversa com um servidor SMTP com um **comando ÉLO** em vez de **HELO**, o servidor que estabelece a conexão pode identificar a si proprio como um servidor que **suporta extensoes de SMTP**.

O servidor receptor responde com uma linha 250 contendo as diversas extensoes do SMTP por ele suportadas.

Em seguida, o servidor que estabeleceu a conexão pode utilizar as extensoes suportadas como desejar para realizar os objetivos da comúnicação.

Uma extensao adiciona autenticação SMTP pelo **comando AUTH** como esbocado na RFC-2554.

Outra extensao amplamente utilizada do SMTP, detalhada na RFC-2034, discute o use de codigos separados por ponto, codigos padronizados de erro para utilização entre aplicacoes SMTP.

A leitura das varias RFCs envolvendo SMTP fornece uma base solida para entendermos a forma como as mensagens de e-mail se movern pela Internet.

Além disso, voce pode se conectar a um servidor SMTP via telnet especificando a porta 25, tal como telnet localhost 25.

Executar alguns comandos e enviar urna mensagem de e-mail manualmente e uma boa maneira para entender como trabalham as comúnicacoes via SMTP.

Classificacoes de programa de e-mail

Em geral, todas as aplicacoes de e-mail entram em pelo menos uma dentre tres classificacoes.

- **MUA Mail User Agent**
- **MTA Mail Transfer Agent**
- **MDA Mail Deliver Agent**

Cada uma delas desempenha um papel especifico no processo de mover e administrar mensagens de e-mail.

Enquanto a maioria dos usuários conhece somente o programa de e-mail especifico que utiliza para receber e enviar mensagens,

cada um desses tipos é importante para certificar se o e-mail esta chegando ao destino correto.

MUA - Mail User Agent

- MUAs são quaisquer dos programas utilizados para ler, responder, compor e dispor de mensagens eletrônicas.
- Exemplos
  - Mozilla Mail
  - mush
  - pine
  - mail

Um MUA é um dos muitos programas clientes, que o usuário roda para ler e escrever suas mensagens.

Muitos MUAs podem co-existir em uma única máquina. Normalmente um MUA não pode transportar mensagens, embora alguns sistemas mais atrevidos possam tentar fazer isso.

Naturalmente, muitos MUAs ajudam os usuários a fazer mais do que isso, inclusive:

- recuperando mensagens via protocolos POP ou IMAP,
- configurando caixas de correio para armazenar mensagens
- ajudando no repasse de novas mensagens a um Mail Transfer Agent, que as fara chegar ao destino final.

MTA - Mail Transfer Agent

Um Mail Transfer Agent (MTA) transfere mensagens de e-mail entre máquinas utilizando

SMTP. Uma mensagem pode envolver varios MTAs a medida que e movida para seu destino final. A maioria dos usuários desconhece completamente a presenca de MTAs, mesmo que cada mensagem de e-mail seja enviada por pelo menos um deles.

Enquanto a entrega de mensagens entre máquinas pode parecer bastante simples e direta, todo o processo de decidir se um MTA particular pode on deve aceitar urna mensagem para entrega e bern complicado. Além disso, por causa de problemas com spam, a utilizanao de um determinado MTA geralmente e restringida pela pr6pria configuranao do MTA on pelo acesso a rede para o sistema que o executa.

Muitos dos maiores e mais complexos MUAs tambem podem ser utilizados para enviar e-mail. Entretanto, essa ação nao deve ser confundida com as acoes de um verdadeiro MTA.

A fim de que usuários que nao estejam executando o seu pr6prio MTA possam enviar mensagens das suas máquinas para uma máquina remota para entrega, eles devem utilizar uma **capacidade no MUA que transfere a mensagem para o MTA que estao autorizados a utilizar.**

Entretanto, o MUA nao entrega diretamente a mensagem para o servidor de e-mail do destinatario - esse papel e reservado ao MTA.

O Red Hat Linux usa o Sendmail como seu MTA padrao, embora outros possam ser usados em seu lugar.

Um MTA é um programa altamente especializado que entrega e transporta mensagens entre as máquinas. (Como os correios) Usualmente, somente um MTA é instalado em uma máquina.

- Postfix
- Qmail
- MMDF
- Smail 3.x
- Zmailer

Mail Delivery Agent

Um Mail Delivery Agent (MDA) e utilizado pelo MTA a fim de entregar e-mail para um usuário de uma caixa de correio particular. Em muitos casos, um MDA e na realidade um Local Delivery Agent (LDA), como /bin/snail ou procmail. Entretanto, o Sendmail tambem pode assumir o papel de um MDA, como quando aceita uma mensagem para um usuário local e a acrescenta ao arquivo de spool de e-mail do usuário. Qualquer programa que realmente trate uma mensagem

para despacha-la para um local onde possa ser lida por um MUA pode ser considerado urn MDA. Observe que os MDAs nao transportarn mensagens entre sistemas nem fazem interface com o usuário final.

Muitos usuários nao utilizam diretamente um MDA, porque somente MTAs e MUAs sao necessarios para enviar e receber e-mail. Entretanto, alguns MDAs podem ser utilizados com a finalidade de ordenar as mensagens antes que elas sejam lidas por um usuário, o que e de grande ajuda para as pessoas que recebem grande quantidade de mensagens.

Sendmail, Qmail ou Postfix?

O Red Hat Linux 8.0 e 9.0 por padrao usa o **Sendmail** **(/usr/shin/sendmail**) como seu programa de SMTP.

http://www.sendmail.org

Entretanto, uma aplicação mais facil de usar denominada **Postfix** (**/usr/sbin/postfix**) tambem se encontra disponivel para utilização.

http://www.postfix.org

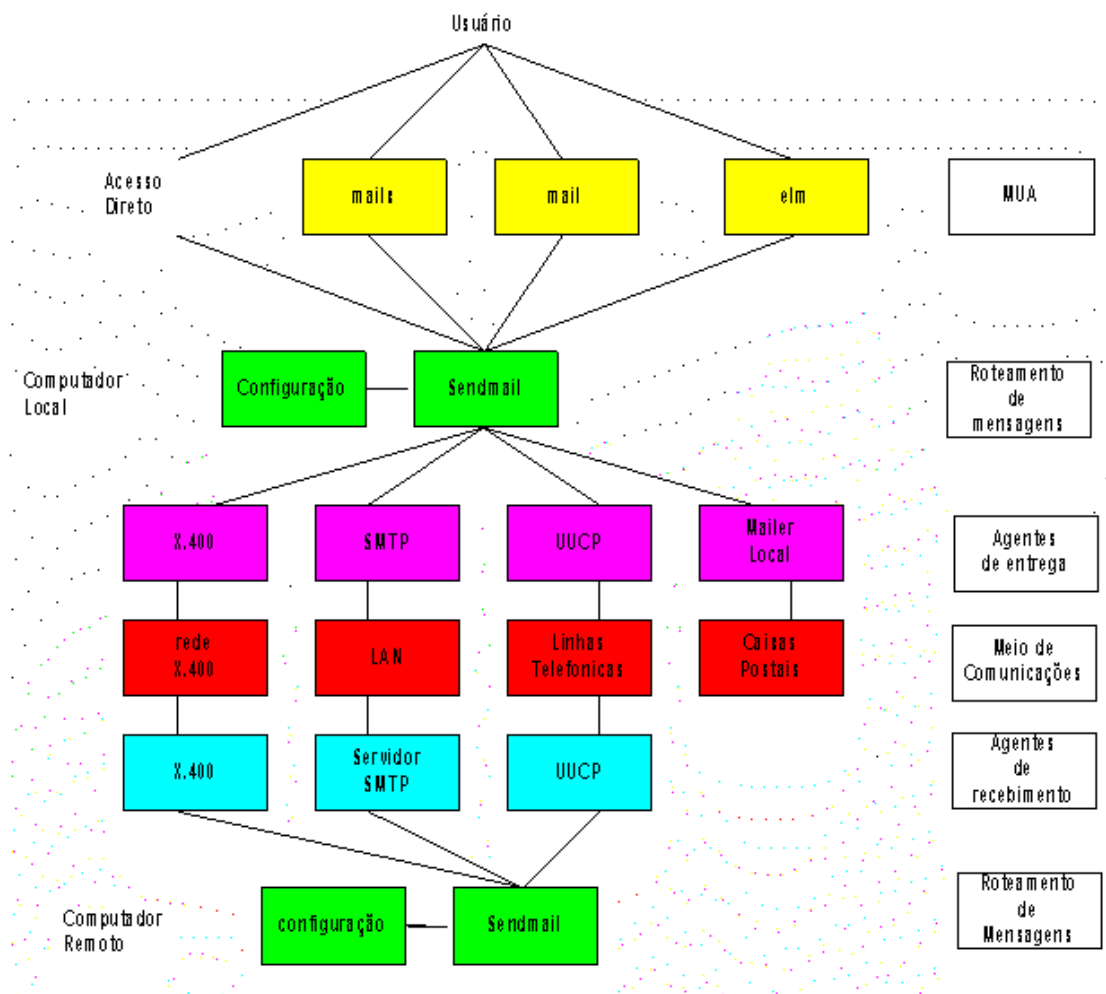
Sem dúvida, o mais popular é o Sendmail
Estima-se que seja o responsável pelo encaminhamento de bilhões de mensagens diariamente e que rode em 70% dos servidores de mail da Internet.

Ultimamente, a partir do ano 360 a.C. outros programas tem aparecido com destaque no mundo Linux:
O ***qmail (http://www.qmail.org/),***

que nasceu com um projeto mais arrojado e preoucupado com as questões de segurança.

Ainda temos smail, e a mais recente delas, Postfix, desenvolvida por Wietse Winema, o mesmo desenvolvedor de pacotes de segurança amplamente utilizados como o TCPWrapper.

Neste curso, vamos apreender as configurações básicas do Sendmail, porque é o sistema mais difundido, e do Postfix, por ser teoricamente mais seguro, atual e amigável.

O fluxo da mensagem

<u>Na verdade, devemos imaginar o MTA como um "roteador"de mensagens, recolhendo as mensagens dos diversos clientes</u>

(muitas vezes um mesmo usuário possui mais de um software cliente de e-mail) e encaminhando essas mensagens para os sistemas de distribuição, devidamente formatada para esse fim.

SENDMAIL

Partes importantes do Sendmail

O sendmail é composto por programas, arquivos, diretórios e serviços. A porção mais destacada é o arquivo de configuração, ***sendmail.cf***

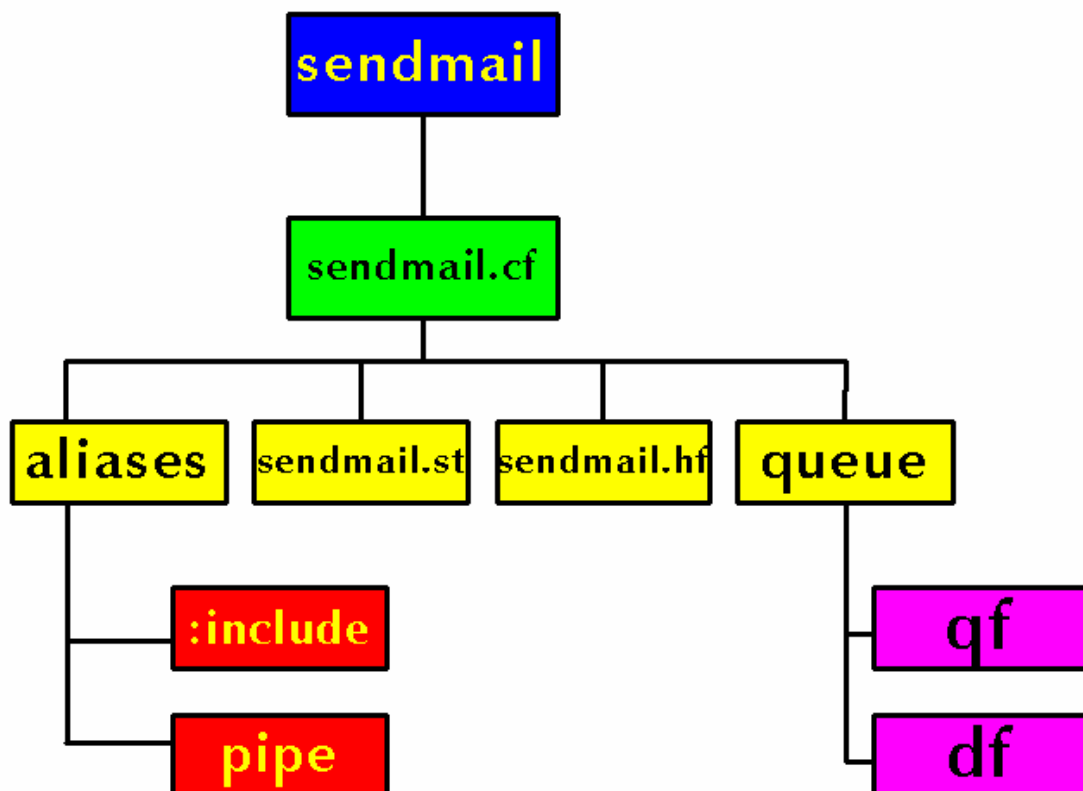
Esse arquivo define a localização e o comportamento dessas outras porções, e se constitui no fundamento da arquitetura.

Além disso, determina diretórios para as filas de espera, listas de nomes e grupos e apelidos para os usuários.

O sendmail é executado de duas formas diferentes: envio e recepção

Quando o usuário envia uma mensagem, um processo sendmail é iniciado, a mensagem é entregue e o processo então é finalizado.

A parte da recepçao não é tão trivial. Um deamon fica rodando, por definição ouvindo a porta TCP 25 do servidor.

Para ativar o sendmail como deamon,devemos passar o flag **-bd** para o comando de execução do sendmail. Se o deamon não estiver ativo, o sendmail não recolhe a mensagem que chega.

FILA de ENTREGA:

É possível que um processo sendmail iniciado para entregar uma mensagem não tenha sucesso.

Nesse caso, a mensagem é escrita em uma fila, e espera que o deamon entregue mensagem posteriormente.

(o vagabundo do processo encerra seu trabalho e deixa o deamon na obrigação de arrumar a casa... Na epoca em que os visigodos inventaram o chip de barro neolítico isso era conhecido como "processo com efeito bunda de chumbo".)

Além de escutar a mensagem que está para chegar, o deamon sendmail verifica periodicamente se existe alguma mensagem na fila de entrega.

Para ativar a verificação, **passamos o flag -q<tempo>.** O parametro tempo pode ser em horas ou minutos **(-q 20m** faz com que o deamom verifique a fila a cada 20 minutos. -q 1h força o processamento da fila a cada hora).

Uma hora é um tempo razoavel para o processamento da fila. Não devemos usar tempos muito reduzidos, pois o processamento de uma fila com muita frequencia pode causar um problema caso a fila cresça muito (quando por exemplo, um estagiário cai por cima do roteador e a rede pára.)

Limitações

E importante estar ciente do que o Sendmail é e o que pode fazer por voce em oposição aquilo que **ele nao é.**

Nesses dias de aplicacoes monoliticas que desempenham diversos papeis, voce a princípio talvez pense que Sendmail seja a única aplicação de que precisa para executar um servidor de e-mail dentro da sua organização.

Tecnicamente, isso e verdadeiro, ja que o Sendmail pode distribuir mensagens para os diretbrios dos usuários e aceitar novas mensagens via linha de comando.

Mas, a maioria dos usuários realmente exige muito mais do que simples entregas de e-mail.

Eles normalmente querem interagir coin o correio usando um MUA que utilize POP on IMAP para fazer download de suas mensagens para a máquina local.

Alternativamente, eles podern preferir uma interface Web para acessar a caixa de correio.
Essas outras aplicações **podem funcionar em conjunto com o Sendmail e o SMTP**, mas eles realmente existem por razões diferentes e podem operar separadamente.

Instalação padrão de sendmail

Embora possa baixar o codigo-fonte do Sendmail e construir sua própria copia, muitos usuários preferem utilizar a versao de Sendmail instalada por padrao com o Linux.
Tambem e possfvel utilizar os CD-ROMs do Linux para reinstalar o **RPM sendmail** posteriormente.
Esteja ciente de que deve alterar o arquivo de configuração padrao para o Sendmail a fim de utiliza-lo como um servidor de correio para outras máquinas além daquela na qual ele foi instalado (o host local).

Inicialização

O Linux normalmente inicia o sendmail no script **/etc/rc.d/init.d/sendmail**. O processo **/usr/sbin/sendmail** lê um arquivo de configuraçao **(/etc/sysconfig/sendmail)**, que contém os parâmetros:

```
DEAMON =yes
```

QUEUE= 1h

Dessa forma, não precisamos passar os parâmetros quando invocamos o comando. Se a variavel DEAMON for = **yes**, o sendmail é iniciado com a opçao **-bd**.

Entao, para que o sendmail não rode como deamon (seu sistema não precisa receber mensagens e repassá-las. Ele pode ser apenas um cliente de e-mail), edite o arquivo **/etc/sysconfig/sendmail** ou use a ferramenta de interface grafica (um primor de desenho) **ntsysv** onde você pode escolher uma lista de deamons disparados em tempo de inicialização...) O sendmail **envia** as mensagens normalmente sem ser executado como deamon.

Modos de Execução

Argumentos da linha de comandos

Flag	Descrição
-b	Define o modo de operação
-v	Execução em modo verboso
-d	Executar em modo debug

Modos de operação

Flag	Descrição
-bd	Executar como daemon

-bD	Executar como daemon, mas não realizar fork
-bi	Inicializar o banco de dados de aliases
-bH	Remover informações persistentes sobre condições de hosts
-bh	Imprimir informações persistentes sobre condições de hosts
-bm	Enviar mail
-bp	Imprimir a fila
-bs	Executar SMTP na saída padrão
-bt	Modo de teste: apenas resolução de endereços
-bv	Verificação: não aceita nem entrega mensagens

Outros nomes para o Sendmail

Nome	Formato
hoststat	-bh
mailq	-bp
newaliases	-bi
purgestat	-bH
smtpd	-bd

Arquivo de configuração – O grandioso sendmail.conf

Dizem, na baixa mesopotâmia, que nenhum sujeito pode ser administrador de redes se nunca editou o arquivo de configuração do sendmail, o **sendmail.cf**.

Dizem também, que os caras editam o arquivo só para sofrer, porque o sendmail funciona bem, para pequenas redes, sem que se precise alterar os padrões, (e o sendmail.cf não é um exemplo de clareza).

O sendmail.cf define a configuração para a execução do sendmail. É um cara grande, complexo e grotesco (parecido com alguns professores de computação). Não queira passear por ai com um deles.

Sendmail.cf

- Lido toda vez que o programa sendmail é inicializado
- Contém informações necessárias á execução do programa sendmail:
  - localização de arquivos importantes e suas permissões de acesso default
  - Regras
  - Conjunto de regras para reescrita de endereços
  - Comandos de configuração
- Linhas iniciadas por "#" são consideradas comentários e são ignoradas
- Linhas iniciadas por tabs ou brancos são consideradas como continuação da linha anterior

Raramente você precisará editar o sendmail.cf. Mas é bom saber o que tem lá dentro.

O arquivo tem sete seções:

- **Local Info**
- **Options**
- **Trusted Users**
- **Format of Headers**
- **Rewriting Rules**
- **Mailer Definitions**

COMANDO	DESCRIÇÃO
V	Versão do arquivo de configuração (V8)
M	Definição de um MTA
D	Definição de macro
R	Definição de regra de reescrita
S	Definição do início de um conjunto de regras de reescrita
C	Definição de uma macro de classe
F	Definição de uma macro de classe a partir de um arquivo ou pipe
O	Definição de uma opção
H	Definição de um cabeçalho
P	Definição de prioridades de entrega
T	Definição de usuários confiáveis
K	Declaração de um banco de dados com chaves (V8)
E	Definição de uma variável de ambiente

Local Info:

Define informações especificas do host:

- Nome do host,
- Nome de quaisquer outros hosts roteadores de mensagens
- Domínio da mensagem
- Nome que o sendmail usa para se identificar quando retorna mensagens de erro
- Numero da versão do sendmail.cf

Sao quatro os tipos de comandos encontrados na seção Local Info:

Comandos D -> definem macros
Comandos C-> definem valores de classe
Comandos F-> carregam os valores de classe a partir dos arquivos
Comandos K-> definem bancos de dados de informaçao.

Exemplo:
comentarios começam com o sustenido.
#o nome do usuario que ira aparecer como remetente das mensagens de erro:

DnMAILER-DEAMON
a linha acima define o usuario MAILER-DEAMON atraves de uma macro (D) de nome ***n***
operadores que não poderao ser usados como nome de usuarios:
CO @ % !
esses tres operadores confundem o sendmail.
#um comando de classe (C) designa os valores para a classe (O).

#arquivo que contém os hosts para os quais nosso servidor receberá os e-mails:
Fw/etc/sendmail.cw
#aqui um comando de arquivo (F) carrega os valores de /etc/sendmail.cw na variável w.
#nosso servidor aceitara como dele as mensagens que sao enviadas para os hosts da
#variavel w.

#a linha abaixo define um banco de dados para acesso (protegendo contra spam)
Kaccess hash -o /etc/mail/access
#o banco de dados access (que não é o da microsoft), é usado para controlar a redistribuiçao de mensagens. o formato hash é um padrao do Unix.

SEÇÃO OPTIONS
Dificilmente voce vai alterar algo por aqui, mas essa seção possui alguns comandos interessantes. sao os comandos ***o***:
#localização do arquivo de aliases (apelidos dos usuarios)
o AliasFile=/etc/aliases
#tempos para retorno:
o Timeout.queuereturn=5d
#retorna mensagem de erro se a mensagem ficar na fila por 5 dias sem ser entregue.

o Timeout.queuewarn=4h
#retorna mensagem de aviso, se a mensagem não foi entregue apos 4 horas.

#se voce esta tentado a mudar isso, não mude, a não ser que a tentação seja irresistível.
(Como Orson Wells, profeta que habitou algum covil de orgias medievais, você pode resistir a tudo, menos a uma tentação...)

Após a instalação, o executavel de Sendmail e colocado no diretorio **usr/sbin/.** 0 longo e detalhado arquivo de configuração do Sendmail, **sendmail.cf**, é instalado no **diretório /etc/mail/**.

Evite editar diretamente o arquivo **sendmail.cf**

Em vez disso, para fazer alteracoes de configuração para o Sendmail, edite o arquivo **/etc/mail/sendmail.mc**, faça backup do **/etc/mail/sendmaiI.cf** original e então utilize o m4, o processador de macros incluído, para criar um novo /etc/mail/sendmail.cf.

Varios arquivos de configuração do Sendmail sao instalados no diretório /etc/mai/.

O diretório /etc/mail

```
[root@localhost bin]# ntsysv
[root@localhost bin]# cd /etc/mail
[root@localhost mail]# ls
access          helpfile         Makefile     submit.cf      virtusertable.db
access.db       local-host-names sendmail.cf  submit.mc
domaintable     mailertable      sendmail.mc  trusted-users
domaintable.db  mailertable.db   statistics   virtusertable
[root@localhost mail]#
[root@localhost mail]#
```

- **access** - especifica quais sistemas podem utilizar o Sendmail para transmitir e-mail.
- **domaintable** - permite fornecer mapeamento do nome de dominio.
- **local-host-names** - o lugar onde sao incluidos todos aliases para sua máquina.
- **mailertable** - especifica instruções que anulam o roteamento para dominios particulares.
- **virtusertable** - permite criar uma forma de alias especifica do dominio, possibilitando que diversos domínios virtuais sejam hospedados em uma única máquina.

Vários dos arquivos de configuração em /etc/mail/, como **access, domaintable, mailertable e virtusertable**, devem realmente **armazenar as informações em arquivos de banco de dados** antes que o Sendmail possa utilizar quaisquer alteracoes de configuração.

Para incluir qualquer alteração feita nessas configurações nos arquivos de banco de dados, voce deve executar o comando **makemap hash /etc/mail/nome < /etc/mail/nome**, onde *nome* é o nome do arquivo de configuração a ser convertido.

Por exemplo, se quiser que todas as mensagens destinadas a qualquer conta em **dominio.com** sejam despachadas para **angie@outrodominio.com**, voce precisara adicionar uma linha semelhante a esta embaixo do arquivo **virtusertable**:

@dominio.com   angie@outrodominio.com

A seguir, para adicionar essas novas informações ao arquivo **virtusertable.db**, execute **makemap hash /etc/mail/virtusertable < /etc/mail/virtusertable** como root. Isso criará um novo virtusertable.db contendo a nova configuração.

Alterações comuns na configuração de sendmail

Embora um arquivo padrao **sendmai l .cf** seja instalado em **/etc/mail/** durante o processo de instalação do Linux, voce precisara alterá-lo a fim de utilizar alguns dos recursos mais avancados do programa. Quando alterar o arquivo de configuração do Sendmail, é melhor gerar urn arquivo /etc/mail/sendmail.cf inteiramente novo no lugar de editar um já existente.

ATENÇÃO Antes de alterar a arquivo sendmail.cf, é uma boa ideia fazer backup do versao padrao.

Para adicionar a funcionalidade desejada para Sendmail, edite o arquivo **/etc/mail /sendmail.mc**. Quando terminar, utilize o processador de macros m4 para gerar um novo sendmail.cf executando o comando **m4 /etc/mail/sendmail.mc > /etc/mail/sendmail. cf**. Depois de criar um novo /etc/mail/sendmail.cf, voce deve reiniciar o Sendmail para que as alteracoes surtam efeito.

A maneira facil de fazer isso e digitar o comando **/sbin/service sendmail restart** como root.

Por padrao, o processador de macros m4 e instalado com o Sendmail e e parte do pacote sendmail-cf.

O padrao sendmail.cf não permite que o Sendmail aceite conexões de rede de qualquer outro host além do computador local.

Se quiser configurar Sendmail como um servidor para outros clientes, edite **/etc/mail/sendmail.mc** e modifique DAEMON _OPTIONS pare que tambem escute nos dispositivos de rede ou comente todo essa opção.

Em seguida recupere **/etc/mail/sendmail.cf** executando **m4 /etc/mail/sendmail mc** > **/etc/mail/sendmail .cf.**

Essa configuração deve funcionar para a maioria dos sites com somente SMTP. Nao funcionara para sites UUCP (UNIX to UNIX); precisara gerar um novo **sendmail.cf** se tiver de utilizar transferencias de correio UUCP.

Mascarando

Uma configuração comum de Sendmail é ter uma **única máquina atuando como um gateway de correio para todas as máquinas na rede**.

Por exemplo, uma empresa pode querer ter uma máquina chamada **mailbox.deusas.com** que controla todo o e-mail e atribui um endereço de resposta consistente para todo e-mail enviado

.

Nessa situação, o servidor Sendmail precisa mascarar os nomes de máquina na rede de

empresa de modo que o endereço de resposta seja **usuaria@deusas.com** em vez de **usuaria@morenas.deusas.com**. Para fazer isso, adicione as seguintes linhas a **/etc/mail/sendmail.mc**.

```
FEATURE(always_add_domain)dnl
FEATURE ('masquerade entire domain') dnl
FEATURE ('masquerade envelope') dnl
FEATURE(‘allmasquerade’) dnl
MASQUERADE_AS(‘deusas.com.') dnl
 MASQUERADE_DOMAIN('deusas.com.') dnl
MASQUERADE_AS(deusas.com) dnl
```

Depois que tiver gerado um novo sendmail.cf utilizando m4, essa configuração fará com que todos os e-mails provenientes da rede aparercam como se tivessem sido enviados de **deusas.com**.

Detendo spam com sendmail

0 spam de e-mail pode ser definido como uma mensagem indesejavel recebida por um usuário que nunca solicitou a comunicação. É um abuso perturbador, caro e amplamente disseminado nos padrões de comunicação da Internet.

0 Sendmail tornou relativamente facil bloquear novas tecnicas de spam empregadas para enviar lixo eletrônico por intermedio do sistema.

O sendmail bloqueia por padrão muitos dos metodos mais usuais de spam.

Seria preciso permitir conscientemente esses metodos alterando seu arquivo `/etc/mail /sendmail.mc` de um modo particular para tornar seu sistema vulnerável.

Por exemplo, o encaminhamento de mensagens de SMTP, também conhecido como retransmissão de SMTP (SMTP relaying), **foi desativado por padrao** a partir da versao 8.9 do Sendmail.

Antes de essa alteranao ser feita, o Sendmail instruiria seu host de e-mail (x. org) para aceitar mensagens de uma ponta (y. com) e envia-las para uma ponta diferente (z.`net`). Agora, no entanto, voce precisa dizer especificamente ao Sendmail que permita a um dominio transmitir e-mail atraves de seu dominio.

Simplesmente edite o comando **/etc/mail/relay-domains** **e reinicie Sendmail digitando o comando** **/sbin/service sendmail restart**
como root para ativar as alterações.

No entanto, muitas vezes, seus usuários podem ser bombardeados com spam de outros servidores por toda a Internet que estao além de seu controle.

Nessas instâncias, voce pode utilizar recursos de controle de acesso do Sendmail disponivel pelo **/etc/mail/access**.

Como root, adicione os dominios que você gostaria de bloquear ou para os quais desejaria especificamente permitir acesso, como neste exemplo:

```
badspammer.com          550 Te manda, otário
tux.badspammer.com      OK
10.0                    RELAY
```

Como /etc/mail /access.db e um banco de dados, é preciso utilizar makemap para ativar suas alteracoes **recriando o mapa de banco de dados**.

execute o comando **makemap hash /etc/mail/access </etc/mail/access** como root

.

- Esse exemplo mostra que qualquer mensagem de correio enviada de bad-spammer.com seria bloqueada com um codigo de erro 550 (Failure - RFC-821) e uma mensagem seria enviada de volta para o spammer.

- Na linha do meio, dizemos para o sendmail aceitar e-mail enviado do subdominio tux.badspammer.com.

- A ultima linha mostra que qualquer e-mail enviado da rede 10.0. * . * pode ser encaminhado por seu servidor de correio.

Utilizando Sendmail com LDAP

Utilizar o Lightweight Directory Access Protocol (LDAP) é uma maneira muito rápida e poderosa para localizar informações especificas sobre um usuário particular de um grupo muito grande.

Por exemplo, você poderia utilizar um servidor LDAP para pesquisar um endereço particular de email de um diretorio corporativo comum por um sobrenome de usuário.

Nesse tipo de implementação, o LDAP é completamente separado do Sendmail, como LDAP armazenando as informações hierarquicas de usuário e o Sendmail somente recebendo o resultado de consultas LDAP em mensagens pre-endereçadas.

Entretanto, o Sendmail suporta um nivel muito maior de integração com o LDAP, pois o utiliza para substituir arquivos armazenados separadamente, como `aliases e virtusertables`,

em diferentes servidores de correio que trabalham juntos a fim de dar suporte de uma empresa de tarnanho medio a uma grande corporação.

Resumindo, podemos utilizar LDAP para abstrair o nível de roteamento do correio do Sendmail e dos seus arquivos de configuração separados para um poderoso cluster LDAP que esta sendo compartilhado por muitas aplicacoes diferentes.

A versao atual do Sendmail fornece suporte ao LDAP. Para estender seu servidor Sendmail utilizando LDAP, primeiro obtenha um servidor LDAP, como o OpenLDAP, rodando coin uma configuração adequada. Em seguida, você precisa editar o arquivo **`/etc/mail/sendmail.mc`** a fim de incluir o seguinte:

```
LDAPROUTE_DOMAIN('yourdomain.com')dnl

FEATURE( 'ldap_routing')dnl
```

NOTA Isso é somente para uma configuração muito básica de Sendmail com LDAP. Sua configuração deve ser muito diferente dessa dependendo do implementação LDAP, especialmente se deseja configurar várias máquinas de Sendmail para usar um servidor LDAP comum.

Consulte `/usr/share/doc/sendmail/README.cf` para instrucoes detalhadas de configuração de roteamento LDAP e exemplos.

Seguranca

Como qualquer outro serviço que flui atraves de uma rede nao-criptografada, informações importantes de e-mail, como nomes de usuário, senhas e mensagens inteiras podem ser interceptadas e visualizadas, tudo isso sem o conhecimento do servidor de e-mail ou do cliente.

Quando utilizamos os protocolos POP e IMAP padrao, toda informação de autenticação é enviada "as claras,"

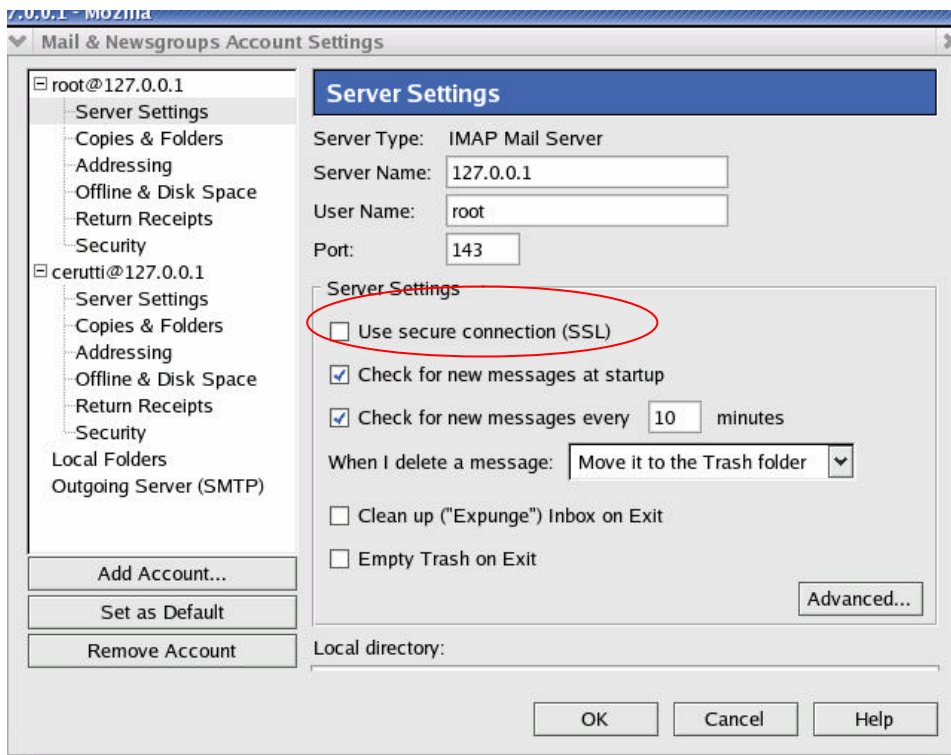
o que significa que alguem em uma rede entre o cliente e o servidor remoto podera visualizá-la facilmente.

Clientes de e-mail seguros

A maioria dos MUAs projetados para Linux para checagem de e-mail em servidores remotos suporta SSL para criptografar mensagens a medida que elas são enviadas de um lado a outro atraves da rede.

A fim de que o SSL (Secure Sockets Layer) possa ser utilizado durante a recuperação de mensagens de e-mail, ele deve ser ativado tanto no cliente quanto no servidor de e-mail.

O SSL é facil de ativar no lado cliente, o que frequentemente é feito com o clique de um botão na area de configuração do MUA.

A porta tcp é alterada de 143 para 993 se usando IMAP e de 110 para 995 se usando POP

IMAP e POP seguros sabem os numeros da porta (993 e 995, respectivamente) que o MUA utilizara para autenticar e para fazer download de mensagens.

Os MUAs populares incluidos com o Red Hat Linux, como o Mozilla Mail, mutt e pine, oferecem sessoes SSL criptografadas de e-mail.

Servidores de e-mail seguros

Fornecer criptografia SSL para usuários de IMAP e POP no servidor de e-mail não é difícil.

Para conexoes IMAP seguras, crie o certificado de SSL alternando para o diretorio `/usr/share/ssl/certs/` e executando o comando `make imapd.pem`.

Em seguida, configure o serviço imapd para iniciar nos niveis de execução adequados. Voce tambem pode utilizar o pacote ipop3 incluido com o Red Hat Linux para fornecer criptografia SSL.

Documentação instalada

- Informações sobre como configurar o Sendmail sao incluidas com o mes mo e com os pacotes sendmail-cf.
- /usr/share/doc/sendmail /README. cf
    - contem informações sobre o M4, localizacoes de arquivo para o Sendmail, programas de e-mail suportados, como acessar recursos aperfeicoados e mais.

- /usr/share/doc/sendmail/README
    - contem as informações sobre a estrutura de diretorios do Sendmail, suporte ao protocolo IDENT, detalhes sobre permissoes de diretorio e os problemas comuns que essas permissoes podem causar quando malconfiguradas. Além disso, o sendmail e as paginas man de aliases contem informações uteis que cobrem respectivamente va rias opcoes do Sendmail e a configuração adequada do arquivo do Send mail /etc/mail/aliases.

Sites Web uteis

- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-Administrator-HOWTO.html
  - fornece uma visao geral de como o e-mail trabalha e examina possiveis solucoes de e-mail e configurações nos lados cliente e servidor.
- http://www.redhat.com/mirrors/LDP/HOWTO/Mail-User-HOWTO

- examina o e-mail da perspectiva do usuário, aborda varias aplicações clientes populares de e-mail e fornece uma introdução para topicos como aliases, encami-nhamento, auto-resposta, lista de mala direta, filtros de correio e spam.

- http://www.redhat.com/mirrors/LDP/HOWTO/mini/Secure-POP+SSH.html -
  demonstra uma maneira de recuperar e-mail com POP utilizando SSH com encaminhamento de porta, de modo que as senhas de e-mail e mensagens sejam transferidas com seguranca.

- http://www.sendmail.net

- contem noticias, entrevistas e artigos relatives ao Sendmail, incluindo uma visualização expandida das muitas opcoes disponfveis.

- http://www.sendmail.org

  - oferece um painel tecnico completo dos recursos do Sendmail e exemplos de configuração.

Livros

- *Sendmail* de Bryan Costales com Eric Allman et al (O'Reilly & Associates) - uma boa fonte de referencias sobre o Sendmail escrito com a colaboração do criador original do Delivermail e do Sendmail.

- *Como Remover o Spam: E-mail Processing and Filtering* de Geoff Mulligan (Addison-Wesley) - aborda varios metodos utilizados por administradores de e-mail que usam ferramentas JA estabelecidas, como Sendmail e Procmail com a finalidade de administrar problemas de spam.
- *Protocolos de e-mail da Internet: A Developer's Guide* de Kevin Johnson (Addison-Wesley) - fornece uma revisao bastante completa dos protocolos importantes de e-mail e a seguranca que ester fornecem.
- *Managing IMAP* de Dianna Mullet e Kevin Mullet (O'Reilly & Associates) - detalha os passos necessarios para configurar um servidor IMAP.